

# PROGRAMME DE LANGLANDS EN BREF

IGOR NIKOLAEV<sup>1</sup>

ABSTRACT. This is a credit mini-course in French prepared for a Summer School at the University of Sherbrooke. The course consists of three one-and-half hour lectures and three credit exercises for a class of advanced graduate students.

## CONTENTS

1. Exposé 1: Programme de Langlands en bref	2
1.1. Grand Théorème de Fermat	2
1.2. Analyse: Groupe modulaire, formes modulaires, etc.	2
1.3. Arithmétique: Courbes elliptiques, points rationnels, etc.	3
1.4. Conjecture de Shimura-Taniyama	4
1.5. Quel est le Programme de Langlands?	4
2. Exposé 2: Analyse des Formes Modulaires	5
2.1. Fonctions automorphes	5
2.2. Formes modulaires de poids $2k$	5
2.3. Points paraboliques du groupe $\Gamma_0(N)$	5
2.4. Formes modulaire paraboliques	6
2.5. Série de Fourier des formes modulaires paraboliques	7
2.6. $L$ -série de formes modulaires paraboliques	7
3. Exposé 3: Arithmétique des courbes elliptiques rationnelles	7
3.1. Courbes elliptiques rationnelles	7
3.2. Rappel des corps finis	8
3.3. Réduction de $E(\mathbf{Q})$ modulo $p$	8
3.4. Fonction zeta de $E(\mathbb{F}_p)$	8
3.5. $L$ -fonction de $E(\mathbf{Q})$	8
3.6. Théorème d'Eichler-Shimura	9
3.7. $L$ -fonctions automorphes et motiviques	9
3.8. Conjectures de Langlands	9
References	9

---

2010 *Mathematics Subject Classification*. Primary 11F70 (représentations automorphes).  
*Key words and phrases*. Courbes Élliptiques, Formes Modulaires.

## 1. EXPOSÉ 1: PROGRAMME DE LANGLANDS EN BREF

**1.1. Grand Théorème de Fermat.** Problème: Comment trouver des solutions à l'équation:

$$X^n + Y^n = Z^n \quad (1.1)$$

ou  $n \in \mathbf{Z}$  et  $n \geq 2$ ?

Si  $X, Y, Z \in \mathbf{C}$  sont nombres complexes, c'est évident:

$$(X, Y, \sqrt[n]{X^n + Y^n}). \quad (1.2)$$

Supposons qu'on cherche solution en corps des nombres rationnels  $\mathbf{Q}$ . Alors, ce n'est pas trivial. (La racine d'un nombre entier n'est pas toujours un nombre entier!)

**Théorème 1.1. (Grand Théorème de Pierre de Fermat, 1601 – 1665)** *Si  $n \geq 3$  alors il n'y a pas de solutions de (1.1) en nombre entier  $(X, Y, Z)$  sauf trivial  $XYZ = 0$ .*

*Proof.* (En bref: **G. Frey, R. Taylor, K. Ribet et A. Wiles**) Considérons la courbe elliptique  $E$  (va être expliqué) donne par équation homogène:

$$E : Y^2Z = X(X - a^pZ)(X + b^pZ) \quad (1.3)$$

telle que:

$$a^p - b^p = c^p, \quad (1.4)$$

ou  $a, b, c \in \mathbf{Z}$  et  $p$  est un nombre premier. Alors (**G. Frey**)  $E$  n'est pas une courbe modulaire (va être expliqué). Alors,

$$a^p - b^p \neq c^p \quad (1.5)$$

et Grand Théorème de Fermat est prouvé!  $\square$

**1.2. Analyse: Groupe modulaire, formes modulaires, etc.** Formes modulaires sont une généralisation des fonctions périodiques.

**Exemple 1.2.** Fonction périodique:

$$(i) \sin(x + 2\pi) = \sin x, \quad \forall x \in \mathbf{C}$$

$$(ii) e^{(2\pi + x)i} = e^{ix}, \quad \forall x \in \mathbf{R}.$$

**Définition 1.3.** Groupe modulaire:

$$SL_2(\mathbf{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbf{Z}, \quad ad - bc = 1 \right\}. \quad (1.6)$$

**Exercice 1.4.** Vérifier que  $SL_2(\mathbf{Z})$  est un groupe multiplicatif; trouver l'unité et l'inverse!

**Définition 1.5.** Groupe de congruence :

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) \mid c \equiv 0 \mod N \right\}, \quad (1.7)$$

ou  $N \geq 1$  est un nombre entier.

**Exercice 1.6.** Prouver que  $\Gamma_0(N)$  est un groupe multiplicatif!

Si  $\mathbb{H} := \{z \in \mathbf{C} \mid \Im(z) > 0\}$  est un demi-plan hyperbolique, alors  $SL_2(\mathbf{Z})$  agit sur  $\mathbb{H}$  par formule:

$$z \mapsto \frac{az+b}{cz+d}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}). \quad (1.8)$$

Le sous-groupe  $\Gamma_0(N) \subset SL_2(\mathbf{Z})$  agit sur  $\mathbb{H}$  et l'espace  $X_0(N) := \mathbb{H}/\Gamma_0(N)$  est une *surface de Riemann* du genre  $g \geq 0$ .

**Exemple 1.7.** Chaque  $N$  définit le genre  $g$  de  $X_0(N)$ ; par exemple:

- (i) si  $N = 2$ , dont  $X_0(2)$  est un sphère, i.e.  $g = 0$ ;
- (ii) si  $N = 11$ , dont  $X_0(11)$  est un tore, i.e.  $g = 1$ .

**Définition 1.8.** Une fonction *automorphe* sur  $\mathbb{H}$  par rapport au groupe  $\Gamma_0(N)$  est une fonction analytique  $f : \mathbb{H} \rightarrow \mathbf{C}$  telle que:

$$f\left(\frac{az+b}{cz+d}\right) = f(z), \quad \forall z \in \mathbb{H}, \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N). \quad (1.9)$$

Une forme *modulaire* de poids égale à 2 est fonction  $f : \mathbb{H} \rightarrow \mathbf{C}$  telle que:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z), \quad \forall z \in \mathbb{H}, \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N). \quad (1.10)$$

### 1.3. Arithmétique: Courbes elliptiques, points rationnels, etc.

**Définition 1.9.** Une courbe elliptique est un cubique de forme:

$$y^2 = x(x-1)(x-\lambda), \quad \lambda \in \mathbf{C}. \quad (1.11)$$

**Exemple 1.10.** Si  $\lambda \in \mathbf{R}$ , alors on peut faire une image graphique, telle que montré à la Figure 1.

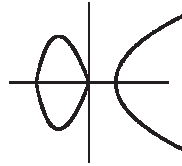


FIGURE 1. Cubique affine  $y^2 = x(x-1)(x+1)$ .

**Exemple 1.11. (Weierstrass)** Si  $\lambda \in \mathbf{C}$ , alors la courbe elliptique est une *surface de Riemann* du genre  $g = 1$ , i.e. un tore complexe.

**Définition 1.12.** Si  $\lambda \in \mathbf{Q}$  alors la courbe (1.11) s'appelle *rationnelle*. Notation:  $E(\mathbf{Q})$ .

#### 1.4. Conjecture de Shimura-Taniyama.

**Théorème 1.13. (Ex-conjecture de Shimura-Taniyama)** *Pour chaque courbe elliptique rationnelle  $E(\mathbf{Q})$ , il existe un nombre entier  $N > 1$ , tel qu'il y a une application holomorphe entre deux surfaces de Riemann:*

$$X_0(N) \rightarrow E(\mathbf{Q}). \quad (1.12)$$

**Définition 1.14.** Si  $E(\mathbf{Q})$  satisfait la condition (1.12) alors  $E(\mathbf{Q})$  s'appelle *modulaire*.

**Corollaire 1.15. (A. Wiles)** *Si une courbe elliptique est rationnelle, alors telle courbe est modulaire.*

Comment peut on prouver le Grand Théorème de Fermat en utilisant le Corollaire 1.15?

**Théorème 1.16. (Grand Théorème de Fermat)** *Si  $n \geq 3$  alors il n'y a pas de solution de (1.1) en nombre entier  $(X, Y, Z)$  sauf trivial  $XYZ = 0$ .*

*Proof.* Supposons  $a^p - b^p = c^p$  est une solution non-triviale pour un nombre premier  $p > 2$ . Considérons la courbe elliptique rationnelle  $E(\mathbf{Q})$  de forme:

$$Y^2Z = X(X - a^pZ)(X + b^pZ). \quad (1.13)$$

Un argument de réduction modulo  $p$  amène à conclusion que  $E(\mathbf{Q})$  n'est jamais modulaire. C'est une contradiction avec le Corollaire 1.15 !

Donc,  $a^p - b^p \neq c^p$  □

**1.5. Quel est le Programme de Langlands?** Robert Langlands, né en Colombie Britannique, professeur à l'Université Princeton (Institute of Advanced Studies).

*Remarque 1.17.* Demi-plan hyperbolique  $\mathbb{H}$  est une *espace homogène* du groupe de Lie  $SL_2(\mathbf{R})$ .

**Exercice 1.18.** Prouver que

$$\mathbb{H} \cong SL_2(\mathbf{R})/SO_2(\mathbf{R}), \quad (1.14)$$

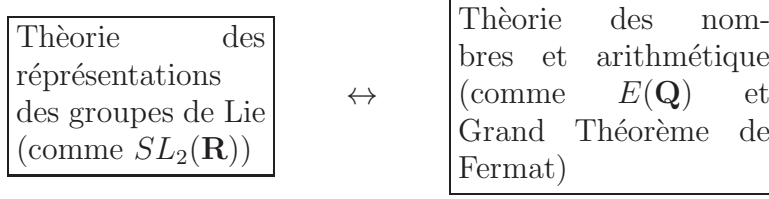
i.e.  $\mathbb{H}$  est une espace homogène. (Conseil: Vérifier que chaque  $z \in \mathbb{H}$  est un point fixe de  $SO_2(\mathbf{R})$  et choisi  $z = i$ .)

Donc, nous avons une application holomorphe:

$$\underbrace{\Gamma_0(N) \backslash SL_2(\mathbf{R})/SO_2(\mathbf{R})}_{\text{groupes de Lie}} \longrightarrow \underbrace{E(\mathbf{Q})}_{\text{arithmétique}}. \quad (1.15)$$

Programme de Langlands en bref.

Motivé par (1.15), trouver les liaisons entre:



À quoi ça sert?

Par exemple, pour prouver le Grande Théorème de Fermat! (parmi d'autre choses)

Dans Exposé 2 et 3 on va détailler le Programme de Langlands.

## 2. EXPOSÉ 2: ANALYSE DES FORMES MODULAIRES

**2.1. Fonctions automorphes.** Fonctions automorphes sont une généralisation des fonctions périodiques.

**Exemple 2.1.** Fonction périodique:

- (i)  $\sin(x + 2\pi) = \sin x, \forall x \in \mathbf{C}$
- (ii)  $e^{(2\pi+x)i} = e^{ix}, \forall x \in \mathbf{R}.$

**Définition 2.2.** Une fonction *automorphe* sur  $\mathbb{H}$  par rapport au groupe  $SL_2(\mathbf{Z})$  est une fonction analytique  $f : \mathbb{H} \rightarrow \mathbf{C}$ , telle que:

$$f\left(\frac{az+b}{cz+d}\right) = f(z), \forall z \in \mathbb{H}, \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}). \quad (2.1)$$

**2.2. Formes modulaires de poids  $2k$ .**

**Définition 2.3.** Une forme *modulaire* de poids  $2k$  par rapport au groupe  $\Gamma_0(N)$  est une fonction holomorphe  $f : \mathbb{H} \rightarrow \mathbf{C}$  telle que:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z), \forall z \in \mathbb{H}, \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N). \quad (2.2)$$

*Remarque 2.4.* Chaque forme modulaire de poids  $2k$  correspond à  $k$ -forme holomorphe sur la surface de Riemann  $X_0(N)$ . Particulièrement, si  $k = 1$  on a une bijection entre formes modulaires de poids 2 et différentielles holomorphes sur  $X_0(N)$ .

**2.3. Points paraboliques du groupe  $\Gamma_0(N)$ .**

**Définition 2.5.** Point  $x \in \partial\mathbb{H}$  (le “absolu” de demi-plan  $\mathbb{H}$ ) est point parabolique du groupe  $\Gamma_0(N)$  s’il existe  $\alpha \in \Gamma_0(N)$  telle que  $\alpha(x) = x$  est un point unique fixé par  $\alpha$ .

**Exemple 2.6.**

$$\begin{aligned} \frac{ax+b}{cx+d} = x &\iff cx^2 + (d-a)x - b = 0, \\ x_{1,2} = \frac{a-d \pm \sqrt{(d-a)^2 + 4bc}}{2c} &= \frac{a-d \pm \sqrt{(a+d)^2 - 4(ad-bc)}}{2c} = \\ &= \frac{a-d \pm \sqrt{(a+d)^2 - 4}}{2c}. \end{aligned}$$

Mais on a  $x_1 = x_2 = x$ , donc  $|a+d| = 2$  et  $x = \frac{a-d}{2c} \in \partial\mathbb{H}$  est un point unique fixé de transformation:

$$\alpha = \begin{pmatrix} a & b \\ c & -a \pm 2 \end{pmatrix} \in \Gamma_0(N).$$

Particulièrement, points paraboliques du groupe  $\Gamma_0(N)$  sont points *rationnelles* de l'absolu  $\partial\mathbb{H}$ .

Pourquoi les points parabolique sont importantes?

Considérons la surface de Riemann:

$$X_0(N) = \mathbb{H}/\Gamma_0(N). \quad (2.3)$$

Orbites du groupe  $\Gamma_0(N)$  ont un “défait” en point parabolique  $x$ , donc la surface de Riemann  $X_0(N)$  a un “bec” en  $x$  !

**2.4. Formes modulaire paraboliques.** Supposons que  $f(z)$  est une forme modulaire de poids 2 pour le groupe  $\Gamma_0(N)$ , i.e.

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z), \quad \forall z \in \mathbb{H}, \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N). \quad (2.4)$$

**Définition 2.7.** Si  $f(x) = 0$  en chaque point parabolique  $x \in \partial\mathbb{H}$  de groupe  $\Gamma_0(N)$ , alors  $f(z)$  s'appelle une forme modulaire *parabolique*. L'espace de toutes les formes paraboliques est notée par  $S_2(\Gamma_0(N))$ . (En allemand “Spitzform” signifie forme parabolique).

Pourquoi les formes modulaires paraboliques sont importantes?

Selon la Remarque 2.4, chaque  $f(z) \in S_2(\Gamma_0(N))$  correspond à la différentielle holomorphe  $\omega = f(z)dz$  de la surface de Riemann  $X_0(N)$ . Donc les zeros de  $\omega$  coïncident avec les “becs” de  $X_0(N)$ . (Il y a toujours un nombre fini de tel “becs”.) Aussi certains formes  $f(z) \in S_2(\Gamma_0(N))$  ont une série de Fourier très intéressante, voir le prochain paragraphe!

**2.5. Série de Fourier des formes modulaires paraboliques.** Si  $f(z) \in S_2(\Gamma_0(N))$ , alors  $f(x) = 0$  si et seulement si  $x \in \partial\mathbb{H}$  est un point parabolique de  $\Gamma_0(N)$ . On va introduire une variable

$$q = e^{2\pi iz}. \quad (2.5)$$

**Définition 2.8.** Série de Fourier de forme modulaire parabolique  $f(z) \in S_2(\Gamma_0(N))$  est une série:

$$f(z) = \sum_{n=-\infty}^{n=\infty} c_n q^n. \quad (2.6)$$

*Remarque 2.9.* Les coefficients  $c_n$  sont très sensible du point de vue “d’arithmétique” de certaines formes modulaires paraboliques  $f(z) \in S_2(\Gamma_0(N))$ .

**Exemple 2.10. ( $j$ -invariate de F. Klein)** Chaque courbe elliptique possède une  $j$ -invariante qu’est constante de classe d’isomorphisme de courbe elliptique. Le  $j$ -invariante est une *forme modulaire parabolique* (!) avec une série de Fourier:

$$j(z) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \dots \quad (2.7)$$

Petit miracle: les coefficients  $c_n$  de  $j(z)$  sont connectés à l’ordre des groupes finis simples (“sporadiques”) !

## 2.6. $L$ -série de formes modulaires paraboliques.

**Définition 2.11.** Si  $f(z) \in S_2(\Gamma_0(N))$  et  $f(z) = \sum_{n=-\infty}^{n=\infty} c_n q^n$ , alors le série convergente

$$L(s, f) := \sum_{n=1}^{\infty} \frac{c_n}{n^s} \quad (2.8)$$

s’appelle  $L$ -série de forme modulaire parabolique.

*Remarque 2.12.* La série  $L(s, f)$  est une généralisation de la fonction zeta de Riemann:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \quad (2.9)$$

## 3. EXPOSÉ 3: ARITHMÉTIQUE DES COURBES ÉLLIPTIQUES RATIONNELLES

### 3.1. Courbes elliptiques rationnelles.

**Définition 3.1.** Une courbe elliptique rationnelle est un cubique de forme:

$$E(\mathbf{Q}) := \{X, Y, Z \in \mathbf{CP}^2 \mid Y^2 Z = X(X - Z)(X - \lambda Z), \quad \lambda \in \mathbf{Q}\}. \quad (3.1)$$

Points *rationnelles* de  $E(\mathbf{Q})$  sont les triplets  $(X, Y, Z)$  tels que  $X, Y, Z \in \mathbf{Q}$  sont en corps de nombres rationnelles.

### 3.2. Rappel des corps finis.

**Exercice 3.2.** Donnez au moins 4 exemples différents de corps de caractéristique *zero*. Aide: La caractéristique de corps  $F$  est le nombre minimale  $n$  telle que

$$nx := \underbrace{x + x + \cdots + x}_{n \text{ fois}} = 0 \quad (3.2)$$

pour chaque  $x \in F$ . Si  $n$  n'existe pas, alors  $\text{char}(F) := 0$ .

**Exemple 3.3.** Si  $p$  est un nombre premier  $p \geq 2$ , alors le corps avec nombres finis des éléments  $\mathbb{F}_p$  a la caractéristique  $\text{char}(\mathbb{F}_p) = p$ . Preuve:

$$px := \underbrace{x + x + \cdots + x}_{p \text{ fois}} = 0 \text{ mod } p, \quad \forall x \in \mathbb{F}_p. \quad (3.3)$$

### 3.3. Réduction de $E(\mathbf{Q})$ modulo $p$ .

*Remarque 3.4.* Si  $(X, Y, Z)$  est un point rationnel de la courbe elliptique  $E(\mathbf{Q})$ , alors  $(X, Y, Z)$  sont aussi un point de courbe elliptique réduite  $E(\mathbf{Q}) \text{ mod } p$ , i.e. solution d'équation:

$$Y^2Z = X(X - Z)(X - \lambda Z) \text{ mod } p. \quad (3.4)$$

**Définition 3.5.** La courbe élliptique  $E(\mathbb{F}_p)$  définie par l'équation (3.4) s'appelle *réduction* de  $E(\mathbf{Q})$  modulo  $p$ .

*Remarque 3.6.* Le nombre de solutions de (3.4) est toujours fini, i.e.

$$|E(\mathbb{F}_p)| < \infty. \quad (3.5)$$

### 3.4. Fonction zeta de $E(\mathbb{F}_p)$ .

**Définition 3.7.** La fonction zeta de la courbe élliptique  $E(\mathbb{F}_p)$  est

$$Z(u, E(\mathbb{F}_p)) = \exp \left( \sum_{n=1}^{\infty} \frac{|E(\mathbb{F}_{p^n})|}{n} u^n \right), \quad (3.6)$$

ou  $\mathbb{F}_{p^n}$  est une extension de degré  $n$  de corps  $\mathbb{F}_p$ .

*Remarque 3.8.* C'est pas difficile de prouver (en utilisant formule des traces de Lefschetz) que  $Z(u, E(\mathbb{F}_p))$  est toujours convergente et:

$$Z(u, E(\mathbb{F}_p)) = \frac{1}{1 - a_p u + p u^2}, \quad (3.7)$$

où  $a_p = p + 1 - |E(\mathbb{F}_p)|$ .

### 3.5. $L$ -fonction de $E(\mathbf{Q})$ .

**Définition 3.9.** Par  $L$ -fonction de  $E(\mathbf{Q})$  on comprend le produit infini:

$$L(s, E(\mathbf{Q})) = \prod_p Z(p^{-s}, E(\mathbb{F}_p)) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}}. \quad (3.8)$$

*Remarque 3.10. (Birch et Swinnerton-Dyer)* La  $L$ -fonction de  $E(\mathbf{Q})$  engendre "toute" information arithmétique à propos de la courbe elliptique rationnelle  $E(\mathbf{Q})$ . Par exemple, l'ordre de zéro au point  $s = 1$  est égal au *rang* de  $E(\mathbf{Q})$  (Conjecture de Birch et Swinnerton-Dyer).



**3.6. Théorème d'Eichler-Shimura.** Nous savons qu'il existe une application holomorphe:

$$X_0(N) \longrightarrow E(\mathbf{Q}). \quad (3.9)$$

D'autre part, il y a une  $L$ -fonction  $L(f, s)$  attachée à la forme modulaire parabolique  $f(z) \in S_2(\Gamma_0(N))$  sur surface de Riemann  $X_0(N)$ . Selon (3.9), on peut se demander comment  $L(f, s)$  est liée à la  $L$ -fonction  $L(E(\mathbf{Q}), s)$  attachée à la courbe elliptique rationnelle  $E(\mathbf{Q})$  ?

**Théorème 3.11. (Eichler et Shimura)** *Pour  $N > 1$  il existe une forme modulaire parabolique  $f(z) \in S_2(\Gamma_0(N))$  et une courbe elliptique rationnelle  $E(\mathbf{Q})$ , telle que:*

$$L(f, s) \equiv L(E(\mathbf{Q}), s). \quad (3.10)$$

*Remarque 3.12.* La forme modulaire parabolique  $f$  en équation (3.10) s'appelle *Hecke eigenform*; telle forme est unique et invariante par rapport à l'algèbre d'opérateur de Hecke.

### 3.7. $L$ -fonctions automorphes et motiviques.

**Définition 3.13.** La  $L$ -fonction  $L(f, s)$  s'appelle *automorphe*, car il provient des formes modulaires paraboliques attachées à l'espace homogène du groupe de Lie  $SL_2(\mathbf{R})$ .

**Définition 3.14.** La  $L$ -fonction  $L(E(\mathbf{Q}), s)$  s'appelle *motivative*, car il provient de formules de trace de Lefschets attachées à la cohomologie motivique pour la variété  $E(\mathbf{Q})$ ; voir **Alexandre Grothendieck**.

**3.8. Conjectures de Langlands.** La formule (3.10) peut être généralisé à variétés arithmétiques arbitraires. Une des conjectures de Robert P. Langlands est une généralisation profonde à ce sujet.

**Conjecture 3.15. (R. P. Langlands)** Chaque  $L$ -fonction motivique est égale au produit de  $L$ -fonctions automorphes pour certains groupes de Lie (appelés algébrique réductif).

**Exercice 3.16.** Prouver 3.15 !!!

**Rémerciement.** Je remercie Ibrahim Assem pour son invitation à participer à l'École d'Été à l'Université de Sherbrooke.

## REFERENCES

1. S. Gelbart, *An elementary introduction to the Langlands program*, Bull. Amer. Math. Soc. **10** (1984), 177-219.
2. R. P. Langlands, *L-functions and automorphic representations*, Proceedings of the ICM 1978, Helsinki, 1978, pp. 165-175.

<sup>1</sup> THE FIELDS INSTITUTE FOR RESEARCH IN MATHEMATICAL SCIENCES, TORONTO, ON, CANADA.

*E-mail address:* [igor.v.nikolaev@gmail.com](mailto:igor.v.nikolaev@gmail.com)